

equal to or greater than that prescribed in paragraph (a)(1) of this section. When an alarmed area is utilized for the storage of Top Secret information and material, the physical barrier must be adequate to prevent surreptitious removal or observation of the material. The physical barrier must also be such that attempted forcible entry will give evidence of such entry into the area or room. As a minimum the alarm system must provide for an immediate response by a security force to an attempted surreptitious or forced entry.

(b) *Secret and Confidential*. Secret and Confidential material may be stored in a manner authorized for Top Secret; or in a vault-type room, or secure storage room which has been approved in accordance with the standards prescribed in the Subject Manual cross referenced in Department Order 2620.4, or until phased out, in containers described in paragraph (d) of this section.

(c) *Specialized security equipment—(1) One and two-drawer containers*. One and two-drawer security containers which are approved by the General Services Administration shall be used primarily in mobile facilities or in areas where small amounts of classified information are stored. Such containers should be securely fastened or guarded to prevent the theft of the container.

(2) *Map and plan file*. A General Services Administration approved Map and Plan File container has been developed for storage of odd-sized items such as computer cards and tapes, maps, charts, plans, and other classified material.

(d) *Non-General Services Administration approved containers*. In addition to the security containers meeting General Services Administration standards, Secret and Confidential classified information may be stored in a steel filing cabinet equipped with a built-in, three-position, dial-type changeable combination lock; or as a last resort, in an existent steel filing cabinet equipped with a steel lock bar, provided it is secured by a General Services Administration approved changeable combination padlock. If a steel filing cabinet with a steel lock bar is used for Secret information, the procedures in Department Order 2620.4 must be adhered to.

(e) *Sensitive Compartmented Information storage*. Sensitive Compartmented Information will be stored only in accredited facilities which meet approved physical security standards for such material pursuant to Director of Central Intelligence Directive 1/19 entitled, "Uniform Procedures for Administrative Handling and Accountability of Sensitive Compartmented Information" and other applicable Department regulations. When maintained in Sensitive Compartmented Information facilities, classified information may be stored in the same container prescribed for storage of Sensitive Compartmented Information; however, when removed from the Sensitive Compartmented Information facility, the provisions of §17.73 (a) through (d) above apply.

§17.74 Procurement and phase-in of new storage equipment.

Whenever new security storage equipment is procured, it will be from the security containers listed on the Federal Supply Schedule, General Services Administration.

(a) Further acquisition for unapproved security containers or modification of cabinets to bar-padlock type as storage equipment for classified information and material is prohibited. Exceptions may be made by the Department Security Officer, upon written request from the Security Programs Manager concerned.

(b) When a security storage container is acquired, the Security Programs Manager shall ensure that a new combination is set before the container is put into use.

§17.75 Designations of security containers.

There shall be no external marking as to the level of classified information authorized to be stored in a container. However, each vault, secure area or security container shall be assigned a number or symbol for the purpose of identifying what level or category of classified information is stored therein. The number or symbol shall be affixed in a conspicuous location on the outside of the vault or security container. Security Programs Managers shall